Yvonne Hofstetter: Láthatatlan háború. Avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását? Corvina Kiadó, 2020; ISBN: 9789631366822

„A háború a politika folytatása más eszközökkel" – Carl von Klausewitz: A háborúról
„Jogállamban a pénz a fegyver" – József Attila: Gyönyörűt láttam
(És minden, ami pénzen megvehető, és nagyot lehet vele ártani – Osman P.)

A Corvina ajánlójából: „*Yvonne Hofstetter, a mesterséges intelligencia szakértője*, minden politika iránt érdeklődőnek megmutatja, *hogyan ássa alá a digitalizáció* a korábban stabil hatalmi viszonyokat, hogyan szítja az újabb fegyverkezéstől való félelmet és teszi a világ történéseit kiszámíthatatlanná. A 21. században a biztonság rendkívül veszélyeztetett, a béke pedig, amiben élünk, törékeny. *A digitális forradalom stratégiai kihasználása lehetővé teszi ugyanis a világ geopolitikai újrarendezését*: az Amerikai Egyesült Államok, Oroszország és Kína egymással harcol a dominanciáért, Európa pedig keresi a nagyhatalmak között a szerepét. *Régen a védelmen alapult az államok közötti stratégiai egyensúly, ma azonban az offenzíva kerül előtérbe*. Egy hálózati kapcsolatokba rendeződött világban megsemmisítő fegyverré válik a kód. Segítségével érzékeny adatok kémlelhetők ki, kritikus infrastruktúrák szabotálhatók el, a lakosságot pedig kamuhírekkel lehet hergelni – anélkül, hogy hivatalos hadüzenet történt volna. A szerző az eseményeket és a világpolitikát masszívan befolyásoló konkrét példákkal illusztrálja a fenyegető helyzetet." (Kiemelések a recenzió szerzőjétől.) A „kód" itt és a könyvben is nyilvánvalóan az informatikai rendszerek befolyásolására, támadására használható proogramokat jelenti.

„Láthatatlan" háború folyik? A korábban a világuralomért vetélkedő Szovjetunió szétesett, az uralma alatt lévő országok elszakadtak, geopolitikai befolyása összezsugorodott – s mindez anélkül, hogy hagyományos fegyveres háború idézte volna elő a vereségét. Új fegyvernemek alkalmazása hozta el ezt, ami olyannyira felőrölte az erejét, hogy már a talponmaradásra sem volt elegendő, hatalmi és befolyási övezetei megtartására pedig végképp nem. *Azóta is új időknek új minőségű háborúi folynak a világban: a sokféle eszközzel vívott hibrid háborúk, amelyek eszközei között vannak a digitális informatikai technológiák alkalmazásai* is. A sikeresen támadók különféle informatikai eszközök révén fejtik ki ártó hatásaikat, a tömeges befolyásolástól az operációs rendszerek megtámadásával okozott, akár hagyományos fegyveres csapással is összemérhető súlyú károkozásig. A hagyományos fegyvereknek is megjelentek a digitálisan „felokosított" változatai, a távolból történő vezérléstől a többé-kevésbé önálló – és várhatóan mind önállóbb – robotokig. Széles áttekintésű fejezet szól róluk: Fegyverkezési verseny a mesterséges intelligencia területén címmel. „*A modern háborúk mások, néhány esetben olyannyira, hogy a régi NATO-kézikönyveket nyugodtan ki is dobhatjuk*" – idézi mindezekre Hofstetter.

A trieri Jog és Digitalizáció Intézete recenziójából: „*A könyv kulcstétele: a világ és annak konfliktusai a digitalizáció révén mélyrehatóan meg fognak változni, és mi erre (még) nem*

készültünk fel. Hofstetter bemutatja a digitalizáció hatásait a globális hatalmi viszonyokra és az államok közötti konfliktusokra. Ennek során rávilágít a digitális vagy hibrid hadviselés technikai lehetőségeire."

Létfontosságú ugyanakkor felismerni: talán még a Hofstetter-osztályú gondolkodók szintjén is ez a felkészületlenség mutatkozik meg abban, hogy *az alcím pontosítást kíván:* az ismeretlentől, beláthatatlan fenyegetéseitől való félelem hajt abban, hogy a veszélyt, tévesen, a digitalizációban lássuk. A vész azonban nem attól jön, hiszen a digitalizáció csak eszközrendszer, hanem azoktól az erőktől, amelyek használják ezeket az eszközöket. Nem a hangszóró szólítja harcba vagy épp ugratja egymás ellen az embereket, hanem azok, akik a belőle jövő üzeneteket alkotják és terjesztik. Így kell olvasnunk ezt a könyvet, s érteni, hogy ha sok utálatosságot tár is fel, maga a digitalizáció semmiképp sem az; mindazért, amit Hofstetter bemutat, semmiképp sem a digitalizáció a felelős.

Szinte napról igazolódik milyen gyorsan növekszik a *téma aktualitása.* Hofstetter írja itt: „Meg kell még említenünk *a valósággal szembeni legnagyobb kihívást, a deep fakes-t*. Videók és hangfelvételek 'mélyhamisítványai' valódi emberek képét-hangját produkálják, amint olyasmiket tesznek vagy mondanak, amiket valójában sohasem tettek vagy mondtak. A mélyhamisítványok különösen azért alattomosak, mert hajlunk arra, hogy elhiggyük, amit a saját szemünkkel látunk. Ezért jelentenek nemzetbiztonsági problémát: könnyen idézhetnek elő politikai konfliktust, erőszakot vagy diplomáciai bonyodalmakat, embereket rágalmazhatnak meg, hamis bizonyítékként szolgálhatnak." E sorok írásának napjaiban jelent meg a hír, hogy az orosz–ukrán háború közepette az internetre kitettek egy mélyhamisítványt, amelyen az ukrán elnök bejelenti a fegyverletételt.

Innentől szóljon magáért a könyv – minden idézet onnan.

„Amikor hekkertámadásokra derül fény, az emberek és a vállalatok egyaránt szeretik azt képzelni, hogy 18 éves kockafejek indítják őket a hálószobájukból. (Vastagon benne van ebben is a jól eladható szenzációkkal dolgozó média: a tizenéves hekkerek kiugró teljesítményeiről szóló hírek jól vonzzák a közönséget, s az emberekben ez marad meg – Osman P.) A közvélekedés azonban lassan átalakul: *a nyomozók mind gyakrabban állapítják meg, hogy a digitális támadásokat idegen államok kormányainak a megbízásából és hangszerelésében hajtják végre*, amelyek magán közreműködőket vesznek igénybe, hogy a net felhasználásával kémkedjenek, szabotázsakciókat hajtsanak végre, és felforgató tevékenységet folytassanak. A Marriott szállodalánc elleni támadás („*500 millió szállodavendég címét tulajdonították el*, emellett sok hitelkártyaadatot is" írja Hofstetter – Osman P.) állítólag a pekingi rezsim számára kémkedő kínai hekkerek számlájára írható. Peking tagadja a támadásokat – vagyis azt a rendkívül tipikus magatartást tanúsítja, melynek célja, hogy elhatárolja magát az idegen felségterületen végrehajtott törvénytelen akcióktól, és elejét vegye a nemzetközi közösség megtorló intézkedéseinek. Az állami támadások kiszervezése hekkerekhez, internetes trollokhoz és robotokhoz, röviden az állam alvállalkozóihoz, megkönnyíti bármiféle

kormányzati részvétel tagadását." – Másrészt, országok, kormányzatok elleni hibrid támadásoknak is hathatós eszköze őket meggyanúsítani különféle elítélendő cselekedetekért. Valakik loptak a Marriottnál: ez remek alkalom Kínát – vagy ki kit akar épp – megvádolni!

A mai szcenárió: „A digitalizáció nem csak magánéletünket és munkás hétköznapjainkat tartja szilárdan hatalmában, a hadviselés is evolúciójának következő szakaszába lép át általa. [Igazából még halvány sejtésünk sincs arról, mi mindent hozhat ez a szakasz, viszont a már küszöbön álló lehetőségek és fenyegetések széltét-hosszát igen jól jellemzi Hofstetter bevezetője: 'Az internet of everything térnyerése áttekinthetetlenné teszi a 21. századi háború eszközeit, ezért csak tematikus válogatást adok belőlük.' (IoE = minden internetje – Osman P.]

A politika és a katonai erőalkalmazás számára az általános hálózatba szerveződés, folyamatos elérhetőségünk, a kommunikáció gyorsasága és az egyre intelligensebbé váló gépek egyfajta szoft háború hasznos eszközei. (Valójában nagyon is sokfajta háborúé, s hogy az 'szoft' marad-e, és meddig, az egyrészt attól függ, meddig tekintjük a beavatkozást és annak hatásait 'szoftnak', másrészt hogy az így megzavart közegben a felek tudják-e és akarják-e féken tartani az erőszakot – Osman P.) Lehetővé teszik, hogy nyomást gyakoroljanak államokra és azok lakosságára – még olyan stabil hatalmakra is, mint az USA –, de *mégis alacsony szinten tartsák a megtorlás és a helyzet tényleges, forró háborúvá való eszkalálódásának a kockázatát. Ez azonban, mint még látni fogjuk, nem zárható ki maradéktalanul*. Az úgynevezett aszimmetrikus vagy hibrid fenyegetések, amelyek közé a digitális kémkedés, a szabotázs és a szubverzió tartozik, a háború megfizethető helyettesítőivé váltak. (Mármint a hagyományos háborúé, mert ez is háború! S Hofstetter itt még nem is említi a tömegek befolyásolását, irányítását vagy épp szabadjára engedését a rend megzavarásával, a támadó érdekei szerint. Később viszont leírja: 'A Twitter segítséget nyújt forradalmak szervezéséhez és kormányok megdöntéséhez – még ha az efféle felkelések a failed state, a működésképtelen állam állapotához vezethetnek is, ahogyan ezt a 2011-es arab tavasz líbiai történései igencsak egyértelműen példázták.' – Osman P.). Mivel pedig *a digitális támadások olcsóbbak, mint egy forró háború*, egyre több állam – a gazdaságilag gyengébbek, kisebb katonai költségvetéssel, rosszabbul felszerelt csapatokkal rendelkezők, ugyanakkor pedig az új globális pozícióra törők is – buzgón kiveszi belőlük a részét, megzavarva ezzel a fennálló nemzetközi rendet és ennek korábbi egyensúlyát." – Növelve ezzel a régió vagy akár a világ instabilitását.

„Ez az oka, hogy *a 21. századi hadviselés számára egyre fontosabbá válnak az olyan univerzális technológiák, mint a kognitív gépekhez kidolgozott mesterséges intelligencia*. (Fura megfogalmazás: az MI inkább maga a 'kognitív gép' – Osman P.) Néhány nemzet világosan felismerte: a digitális technológiák nemcsak gazdasági hasznot hajtanak, hanem politikai és katonai fölényt is eredményeznek. *Aki megtalálja a digitalizáció geostratégiai bevetési lehetőségeit, vezető pozícióba juthat a nagyhatalmak újkeletű erőpróba-versenyében*." – Valójában kétséges ez a sorrend – vajon tényleg a gazdasági haszonszerzés-e az elsődleges mozgató. Becslések szerint a 20. század technológiai forradalmaiban – legalábbis az internetes óriás-

cégek felívelését megelőzően – az innovációs fejlesztési ráfordítások nagyjából kétharmada a hadiiparba ment, s utóbb onnan kerültek át innovációs eredmények a polgári szférába, gazdasági hasznosításra. Igazából egyre nehezebb lesz megmondani, minek is tekintendők ilyen megközelítésben az új digitális technológiák: elsődlegesen hatalom- vagy haszonszerzési eszközöknek. Minél inkább az információs térben zajlik az országok, közösségek, úgyszintén a gazdaságok és azok szereplőinek élete, annál bonyolultabb e fontossági sorrend kérdése. Különösen élessé válik ez azon az új és várhatóan rohamosan növekvő jelentőségű csatatéren, amelyet Hofstetter rögtön az itt következőkben felhoz: a *minden internetjén*.

Az új szcenárió (és harctér): „*Az Egyesült Államok,* amelynek vezető digitális hatalmi státuszát eddig senki sem kérdőjelezte meg, *azt tapasztalja most, hogy egykor volt előnye rohamosan fogy, befolyása pedig erőtől duzzadó felkapaszkodottak – különösen Kína – javára csökken*. Amerika visszavonulása és az a vehemencia, amivel a vetélkedő hatalmak térben terjeszkednek, egy olyan új, ijesztő fegyverkezési verseny nyitányát jelenti, amely nem korlátozódik pusztán adatlopásra, szabotázsra és felforgatásra. A digitális fegyverkezési verseny azáltal, hogy az internet of everything (IoE, minden internetje) megjelenésével minden mindennel hálózatba kapcsolódik, *hatalmába keríti a fizikai világot is*, amely még okosabb lesz, mint az okostelefonjaink, okosházaink vagy okosautóink: elterjednek a harci robotok, a drónrajok, az intelligens implantátumok, a hálózatba kötött nukleáris fegyverek és az intelligens muníciót szállító hiperszonikus hordozóeszközök." – S nem hagyható itt említetlenül: *az IoF egyben sebezhetővé is tesz mindent*, amihez általa hozzá lehet férni. *A digitális támadók, másrészt az ellenük védekezők így mindinkább e láthatatlan háború legfontosabb elitalakulatai közé kerülnek*.

A könyv áttekintése Hofstettertől:
„*Az 1. fejezet azzal kezdődik, hogy az államok digitális módszerekkel kémkednek és szabotálnak*. A hasonló, de nem állami szereplők – például bűnözők vagy terroristák – által önös érdekből végrehajtott műveletek kérdését tudatosan figyelmen kívül hagyjuk, mert azon szeretnénk elgondolkodni, hogy vajon csakugyan háború-e az, amit mi különösebb megfontolás nélkül 'cyberháborúnak' nevezünk. (Felettébb érdekes: ha már digitális módszerekkel történő kémkedésről van szó, a gazdaság szereplőit miért nem említi a szerző? A kisebb országoknál erősebb óriásvállalatok, másrészt a gazdasági hatalom és az állami vezetés nem ritka összefonódásai korában olykor elég nehéz lehet eldönteni, hol is húzódnak a frontvonalak. S vajon tényleg elképzelhetetlen, hogy a gazdasági konkurenciaharcban akár még az ellenfél működésének akadályozását is bevetik? Fontos kérdés az is, vajon szabad-e a terroristák cselekvését pusztán önös érdekeknek betudni – ez jócskán nehezíti a megértésüket – Osman P.)

A háború nemzetközi jogi definíciója kifejezetten megköveteli előfeltételként, hogy államok közti cselekvésre kerüljön sor. Ha azonban az erőszak nem állami tényezőktől, például szabadságharcosoktól, felkelőktől, terroristáktól vagy állami megbízatással nem rendelkező

privát hekkerektől indul ki, a szó szoros értelmében véve nem teljesül a fenti nemzetközi jogi követelmény." – Ez roppant csúszós terület, és meglehetősen behatárolhatatlanná teszi e téma tárgyalását! Eleve, Hofstetter „erőszakot" ír, de mi van az olyan ráhatásokkal, amelyek akárcsak közvetve, a következményeik révén válthatnak ki erőszakot? „Állami megbízatással nem rendelkező" – miként bizonyítható az ellenkezője? Melyik állam elég bolond rábizonyítható megbízást adni ilyesfajta tevékenységre más államok ellen? Hogyan bizonyítható az állami indíttatás, ha közbenső aktorok vannak? Valóban morcos helyi erők támadnak-e, vagy külföldi indíttatásúak? Egyáltalán, a hibrid hadviselésben mi minősül háborús támadásnak? Pl. miként választható el hitelesen a jogos elégedetlenség megnyilvánulása az ország kormányzatának gyengítését szolgáló zavarkeltéstől, belpolitikai beavatkozástól? Tisztán helyi(nek mutatkozó), illetve nyíltan nemzetközi hálózathoz kapcsolódó civil szervezetek, nemzetközi szervezetek helyi filiáléi igen sokrétű, átláthatatlan áttételt képezhetnek támadó és megtámadott között. Hibridháborús cselekmény-e beavatkozni egy ország belpolitikájába az egyik fél oldalán? Különösen az-e belső konfliktusok szítására, vagy épp billegő helyzetben, amilyen a választások időszaka? Ha igen, minek tekintendő az ország valutája elleni támadás, amit természetesen gazdasági érdekek is hajthatnak, de komoly támadási lehetőséget ad a regnáló kormányzat ellen is? S rögtön az itt következőkben Hofstetter rátér az információs hadviselésre.

Hofstetter fejtegetései helyenként egyértelmű politikai oldalválasztást mutatnak – ezt csak azért említjük, mert ez olykor a tényállításaiban is megjelenik. „Háborús vagy békeidőkben a hatalom kontrolljának állandó velejárója annak a bizalomnak az aláásása, amivel egy adott népesség a kormánya iránt viseltetik. Az efféle felforgatás mesterműve volt, ahogyan 2016-ban Moszkva koordinált támadásokkal ásta alá az amerikai elnökválasztási kampányt, amit Robert Mueller amerikai különleges ügyész vizsgált és ismertetett igen alaposan. A szubverziót a Facebook, a Twitter és társaik üzleti modelljei tették lehetővé. *Az, hogy a 21. század információs tere miképpen osztja meg a társadalmat, és hogyan szolgál táptalajul a demagógok felemelkedéséhez, a 2. fejezet elmélkedéseinek a tárgya*."

Itt álljunk meg egy kis elgondolkodásra. Hofstetter „a 21. század információs teréről" beszél, mi pedig tanúi és részesei/elszenvedői vagyunk, miként fonódik össze különféle spontán vagy épp nagyon is irányított hatások eredményeként ez az információs tér a társadalom és a gazdaság egyéb tereivel. A Meta cég meg is hirdette a Metaverzum koncepciót, amely lényegében már évek óta egyre inkább működő valóság. Az emberekhez mindinkább ebben az információs térben jutnak el a gondolkodásukat, cselekvéseiket és döntéseiket befolyásoló vagy már irányító információk és hatások. Ez talán többé-kevésbé még úgy is vehető, mint a korábbi befolyásolási technológiák szerves fejlődésének jelenlegi stádiuma. A minden bizonnyal sorsdöntő minőségi ugrás azzal következett be, hogy az országok vezetései a társadalommal – és valamelyest a külvilággal – folytatott, különböző szintű kommunikációjuk nagy részét átvitték a nagy, globális közösségi hálókra. Ezek a hálók azonban óriási gazdasági erővel bíró magáncégek tulajdonában vannak, amelyek nemcsak teljes rendelke-

zési jogot gyakorolnak felettük, hanem még a saját „irányelveiknek" megfelelően „moderálják" – magyarán cenzúrázzák – is az ott folyó kommunikációt. Ez olyan hatalmi pozíciót ad e hálók működtetőinek, amilyet hagyományos cégek vezetőiről elképzelni sem lehetett. A hírek szerint ez a cenzúra valamilyen mértékben még az USA hivatalban lévő elnökét is többször elérte. Az alapvető kérdés, amelyért ez idekívánkozott, a szuverenitásé: miként érinti országok vagy bármilyen más közösség, szervezet szuverenitását, ha a vezetőik és a társadalom közötti kommunikáció magáncégek ilyen hatalma alatt folyik? Ha tovább is visszük a gondolatmenetet, miként érintheti az országok nemzetbiztonságát, ha vezetőik, kormányzataik nyilvános megnyilatkozásaiba a kommunikációs csatornák tulajdonosai így beavatkozhatnak, méghozzá az adott rendszerben teljesen legálisan? S nyilvánvalóan következik az a kérdés is, hogy milyen kitettségeket hoz létre ezeknek az információs rendszereknek a támadhatósága.

A *3. fejezet* a virtuális világot elhagyva kilép a pusztító autonóm fegyverrendszerek fizikai valóságába. Nem csak Németország akarja 19. törvényhozási időszakának koalíciós szerződése értelmében 2021-ig törvényen kívül helyezni a letális, azaz emberélet kioltására alkalmas autonóm fegyverrendszereket (Hofstetter ezt 2019-ben írta – Osman P.): más államok is küzdenek ezeknek a fenyegető, új eszközöknek a szabályozásáért, amelyek a semmiből felbukkanva aktiválják kill cycle-jukat (többelemű csapásmérő akciósorukat), és emberi közreműködés nélkül képesek ölni. *Betiltásukra azonban kevés az esély*, azért is, mert Németország nem akarja szabályozni azt, ami saját felfogása szerint még nem létezik: azokat az autonóm fegyvereket, melyeknek döntő funkcióira az ember már semmiféle hatással nincs. *Lehetséges, hogy ekképpen a tilalom megvalósulása talán nem is a jogban, hanem az elektronikus hadviselés területén végrehajtandó magasabb szintű ellenintézkedésekben keresendő?*

„*Akit digitális támadás ér, az lehetőleg bosszút akar állni*. (A végletesen félénkektől vagy megfélemlítettektől eltekintve, nagyjából mindenki első reagálása, hogy a támadásért visszavág. Bölcsebbek folytatják annak mérlegelésével, megéri-e ez a ráfordítást, másrészt várhatóan mit hoz a fejére, ha megteszi, vagy épp ha nem teszi meg. Mindkettőnek megvannak a többnyire előre biztosan fel nem mérhető kockázatai – Osman P.) 'Ha egyszer egy ilyen hekker a kezem közé kerül, én kitekerem a nyakát!', hallom józan, komoly programozóktól, akik digitális támadások következményeképpen újra meg újra plusz munkafeladatokkal szembesülnek. Emiatt aztán *egyre több vállalkozás óhajt saját hacking back potenciált kialakítani. De vajon egyáltalán megengedett-e a visszahekkelés?* Vajon a megtorlás csakugyan a valódi támadót éri utol – vagy netán egy vétlen szereplőt valamely szövetséges országban, akinek csak visszaéltek a számítógépével egy támadás céljából? És ha mondjuk a hacking back megengedett, *vajon a védekező fél készült egy eszkaláció következményeire is?* A digitális támadások elleni védekezés kényes politikai ügy, és komoly diplomáciai bonyodalmakat okozhat. *Azt, hogy a nemzetközi jog hogyan áll a digitális idők védelmi kérdéseihez, a 4. fejezetben taglaljuk*." – Biztosra vehető, hogy ha a visszatámadáshoz, megtorláshoz alkalmazott

eszközök törvénysértők, akkor az alkalmazásukat nem teszi legálisabbá az sem, hogy támadásra válaszoltak velük.

„Ha némelyik állam felismeri, hogy a digitális korszak technológiái a geopolitikájukat is támogathatják, technológiastratégiájukat is eszerint alakítják majd. Amint az *5. fejezetben* megállapítjuk, *a digitális stratégiákat illetően vannak különbségek a Nyugat, illetve Kína és Oroszország között. Különösen a mesterséges intelligenciát, a 21. század kulcstechnológiáját alkalmazzák eltérően az országok politikai rendszerük függvényében* – itt a nagyobb gazdasági versenyképesség érdekében, ott a gazdasági szempontból releváns források politikai és katonai ellenőrzése céljából. A mesterséges intelligencia felhasználásának különbségei abból adódnak, hogy két eltérő rendszeralternatíva ütközik első alkalommal össze: a neoliberalizmus és a világuralomról szőtt kínai álom." – Bár igazán erős megilletődöttségre kötelez, hogy Hofstetter még a Chatham House – más néven Royal Institute of International Affairs – Demokrácia és Technológia Bizottságának is tagja, nem hagyható említetlenül, hogy ebben az összegzésben erős leegyszerűsítésnek tűnő állítások is megjelennek. Már önmagában az is, hogy a digitális stratégiák tekintetében a geopolitikák közti különbségekként csupán két ellenpólust emel ki, egybevonva Kínát és Oroszországot – a 21. századnak aligha csupán e három lesz a meghatározó geopolitikai szereplője. India mindössze annyival szerepel az egész könyvben, hogy „a világ legnagyobb – noha működési zavarokkal küszködő – demokráciája", jóllehet potenciálja nagyon is magasra röpítheti az eljövendő geopolitikai ranglistán. A jövőbeli kilátások vonatkozásában szintén nagyon nem eleve elhanyagolható Brazília mindössze ennyit kap: „elnökké választotta a maga Donald Trumpját". „Két eltérő rendszeralternatíva" sem első alkalommal ütközik meg a globális csatatéren, s a mesterséges intelligencia felhasználását sem igazán az itt említett tényezők uralják. „Amerika és a profit logikája" az említett 5. fejezet egyik idevágó alcíme, a valóság azonban az, hogy az USA meg sem engedhetné magának, hogy katonai potenciáljának folyamatos fejlesztése a háttérbe szoruljon. A 21. századi Kínára sem épp az tűnik jellemzőnek, hogy álmokat szőne, még kevésbé, hogy az ideológiát helyezné a nagyon is gyakorlatias célok elérése fölé. S alighanem kétely nélkül kijelenthető, hogy mindkét „rendszeralternatíva" országai egyaránt igyekeznek mindent kihozni az MI fejlesztéséből és felhasználásából mind katonai potenciáljuk erősítésében (az ország méretéből és erejéből következő geopolitikai törekvéseik szerint), mind pedig a gazdaságaikban. Ami pedig az itt így aposztrofált Nyugatot illeti, némi merészséggel még az a kérdés is felvethető, vajon az említett neoliberalizmus ura-e vagy inkább eszköze a tőkés termelési mód jelenlegi paradigmájának.

„*A két rendszeralternatíva között elhelyezkedő Európa kihívásokkal kénytelen szembenézni*. Mit jelent vajon az új, ázsiai nagyhatalmi törekvés a mi európai földrészünk számára? Donald Trump Amerikája (Hol van az már! – Osman P.) mindenesetre nem száll síkra már Európa biztonságáért. *A kontinens így még inkább csak magára számíthat* a nyomással és a megosztó törekvésekkel szemben, amelyek a – közelebbi és távolabbi – Kelet részéről érik. *Vajon képes-e Európa saját világpolitikát megfogalmazni és eszerint élni? Az új technológiák*

ebben segítségére lehetnek. Ezzel kapcsolatos elgondolások kis választékával szolgál a *6. fejezet*."

Némileg furcsa: ha a Nyugatot és a neoliberalizmust tekintjük az egyik rendszeralternatívának, miért választja le róla Hofstetter Európát? S hogy *milyennek látja és láttatja ehhez Európát*, azt jellemzi az itt következő idézet. „*Európa is válságban van, és minden, csak nem egységes*. Nagy-Britannia úgy döntött, hogy kilép az Unióból, s a továbbiakban egymagában áll. *A keleti bővítés országai alig rendelkeznek integratív erőkkel, és az illiberális demokrácia koncepciójával, a sajtószabadság és a független igazságszolgáltatás korlátozásával magukat az Unió politikai alappilléreit támadják*. (Vajon erre a jellemzésre mennyire áll meg minden tudományos igényű elemzés alapkövetelménye, a 'sine ira et studio', azaz 'harag és részrehajlás nélkül'? – Osman P.) Skandinávia, amely a világ tökéletes demokráciáinak listáján előkelő helyet foglal el, speciális eset, meglehetősen higgadt és legtöbbször sikeres a szociális érdekek kezelésében. *Egy negyedik európai régiót alkot az ún. Mag-Európa*, amely az Unió alapeszméjének értelmében továbbra is még békésen, egységesen, vagy legalábbis kompromisszumokra készen akar együtt élni, nem mentes azonban a szociális feszültségektől és társadalmi megosztottságtól. Franciaországban a sárgamellényesek demonstrálnak a reformok ellen, egész Európában előretörőben van a jobboldali populizmus, *a digitalizáció pedig súlyos szociális gondokkal fenyeget azokon a helyeken, ahol a munkát automatizálják, vagy pedig a technika gyorsabban terjed, hogysem az emberek megtanulhatnák, hogyan bánjanak vele*." – „Megtanulhatnák"? Nagyon úgy néz ki, hogy az utóbbi évtizedek egyik legfontosabbá vált koncepciója, az élethosszig tanulás már a közeljövőben mind több ember számára a túlélés alapvető eszköze lesz abban a versenyfutásban, amely az emberek és a robotok között bontakozik ki a munka világában, legalábbis a tőkés termelési rend mai paradigmájában. Más irányba terelő külső kényszer nélkül a tőke ebben a maga érdekeit követi, ami pedig azt hozza, hogy robotokat alkalmazzon mindenütt, ahol ez számára kifizetődőbb az emberek alkalmazásánál. Ezt már az MI és a velejáró negyedik ipari forradalom előtti korokban is láttuk, a jól automatizálható munkaelemek és -folyamatok automatizálásában. Ahogy pedig fejlődnek a robotok, úgy állíthatják őket rendszerbe mind fejlettebb tevékenységek végzésére, ami szükségképp az emberek kiszorulásával is jár onnan. Talán nem túl merész feltevés, hogy ezzel a digitalizáció előbb-utóbb egy új paradigmát kényszerít majd a társadalmakra és az azok alapjául szolgáló gazdaságokra. Ehhez a fejezet egyik alcímét emeljük ide: „Bátorság a határozott demokráciapolitikához".

„Amikor a politikai hatalom és a katonai erőszak kontextusában kezdtem foglalkozni digitális technológiákkal, nyomban a gondolkodás látszólag leküzdhetetlen akadályába ütköztem. Akinek jobb fegyvere van – mondaná az ember elsőre reflexszerűn –, az fog érvényesülni politikailag vagy katonailag. (Ez eleve nem igaz! A fegyver szükséges, de messze nem elégséges eszköz a harccal kivívott győzelemhez. A lehető legjobb használatához szükséges tudás nélkül mit sem ér, a nagyobb tudás viszont még gyengébb fegyverrel is képes lehet győzni a másik felett. Ez a tudás pedig a kardforgató technikai képzettségétől, harci

tapasztalatától, hidegvérétől és lélekjelenlététől ma már a legbonyolultabb hibrid fegyverrendszerek maximális hatékonyságú felhasználásához szükséges technológiákig terjed, s természetesen minél bonyolultabb, magasabb technikai színvonalú a fegyver, annál több kell hozzá belőle is – Osman P.) Csak lassan tárultak fel előttem a világrend szemünk előtt zajló rendkívüli átrendeződésének a politikai finomságai, és vált világossá a folyamat jelentősége. *Lélegzetelállító dolog történik, és arra vár, hogy észrevegyük, tudatosítsuk és tematizáljuk. A technológia pedig nem pusztán mellékszereplő, hanem az egyik, ha nem a legfontosabb kulcstényező abban, hogy miféle rend uralja majd ezt a mi digitális 21. századunkat*." – Jókait idézve (A kiskirályok): „Tagadok aztat". Amíg az önfejlesztő általános MI a fekete disztópiák jóslatainak megfelelően át nem veszi az uralmat a világ felett, a rendet meghatározó kulcstényező mindig az lesz, hogy mit akarnak maguknak teremteni a technológiákkal azok urai, vagyis az emberek valamiféle szervezetei, ma leginkább a nagyvállalatok. Ezek működtetik a technológiákat, s az e működésekből következő gazdasági és társadalmi hatások alakítják a 21. század rendjét – erősen meglehet, hogy akár működtetőik szándékától eltérően is, de a technológiák, a mondott határig ebben csak eszközök maradnak.

Nézzünk bele egy kicsit a részletes kifejtés elejébe, a fejezetcím és alcímek segítségével:

- *A kód mint fegyver* – Benne, egyebek közt: *Biztonsági rések*– programhibák, amelyek útján be lehet hatolni a rendszerbe. Hofstetter példaként hozza a hírhedt WannaCry zsarolószoftvert, amely rohamosan terjedt el, és 99 országot fertőzött meg. A történet igen sokat elmond témánk sajátosságairól, ebből idézünk: „Nemcsak az NSA (Amerikai Nemzetbiztonsági Ügynökség – Osman P.), hanem más nyugati biztonsági szervezetek is gyűjtik a számítógépes programok biztonsági réseit, hogy szükség esetén betörhessenek a világ bármelyik számítógépébe. A biztonsági réseket normális körülmények között szigorú titoktartás övezi, ám az NSA maga is hekkertámadás áldozatává vált." Ebből lett a WannaCry. „Kínát és Oroszországot szokták elsőként gyanúsítani a hekkertámadások 'szerzőségével', ám kiderült, hogy Észak-Korea áll a WannaCry-os cybertámadás mögött. Egy állam és hekkerei támadást intéztek számos más állam ellen." – A kapcsolat az állam és a hekkerek között többnyire nem bizonyítható, de maga az állítás is jó propagandafegyver ebben a háborúban.
- *Két út a hatalomhoz*: „Amikor a 21. században olyasmi válik fegyverré, ami nem tartozik a korábbi évtizedek klasszikus fegyverarzenáljába, mert újfajta technikát képvisel, ideje reflektálnunk rá, hogyan változik meg a háború természete a digitalizáció révén, és hogyan kérdőjeleződik meg alapvetően a háborúval és békével kapcsolatos felfogásunk."
- *Elkötelezettség a béke iránt*: „A béke elmélyítésének célja alighanem igencsak európai eszme. Így a katonai erőszak elutasítása is a hadviselés kulturálisan meghatározott, etnocentrikus megközelítése. *Más kultúrákra ugyanis egyáltalán nem érvényes, ami*

iránt Európa olyannyira elkötelezettnek érzi magát. Ezt Angela Merkel külügyminisztere, Sigmar Gabriel így fogalmazta meg: 'Egyetlen vegetáriánusként átkozottul nehéz dolgunk lesz a húsevők világában.'"

Idetolakszik a megjegyzés: ez a „béke" leginkább a hagyományos fegyverekkel vívott háború hiányát jelenti, s a napi gyakorlat jól mutatja, hogy messze nem zárja ki a hibrid fegyverek alkalmazását. Erről szól a következő idézet is. „A hidegháborúra, amelyben hallgattak az atomfegyverek, a terror elleni háború következett, most pedig a 'cyberháború'. Állandóan együtt élünk egy diffúz fenyegetéssel és azzal a lehetőséggel, hogy az erőszak egy napon váratlanul, kézzelfogható formában manifesztálódik, és bármelyikünket elérheti. Akkor hát a hatalmat és az erőszakot, a békét és a háborút mégsem tudjuk élesen elhatárolni egymástól. Ehelyett a két szituáció közti tartósan zavaros állapotban élünk – egy hibrid helyzet kontinuumában."

– *A környezeti intelligencia mint csatatér*: „Egyre több szereplő van fenn a neten és vesz részt a mindennapi életben, szünet nélkül interakciókat folytatva és kommunikálva. Ez zajlik a minden internetjén. A jogtudomány az általános hálózatiságot és ennek hétköznapi objektumok révén adódó kognitív potenciálját környezeti intelligenciának nevezi. Az emberek, a gondolataik, a szándékaik, a pszichéik és tárgyaik hálózata ily módon napról napra értékesebb lesz, a hálózat növekedésével pedig egyre kívánatosabbnak tűnik a környezeti intelligencia politikai és katonai célú felhasználása a geopolitika eszközeként. E jövőbeli csatatéren – a szereplők szándékai szerint – a cél az irányítás átvétele vagy már létező államhatalmak és társadalmi struktúrák további fenntartása, a demokráciáé éppúgy, mint a diktatúráé. A társadalom közösségi megakomputerré való átalakítása, úgy tűnik, lehetővé teszi, hogy lemondjunk a klasszikus katonai eszközökről, és mégis folytassunk háborúkat. A digitalizáció a hatalom és az erőszak újfajta eszközeit teszi lehetővé."
– *Hibrid hadijátékok*: „Az államok nem csak katonai vállalkozásokra támaszkodnak, ha ki akarják szervezni háborúikat. Azok körébe, akiket egy kormány igénybe vehet, beletartoznak bűnözők, hekkerek, kémek, újságírók is, továbbá mindazok, akik be akarják hízelegni magukat a kormányuknál. A digitális korszakban kamatoztatják képességeiket, legyen szó akár információk gyűjtéséről, propaganda internetes terjesztéséről, adatlopásról, vagy ransomware, zsarolóprogram segítségével elkövetett zsarolásról. A magánszektor ebben a vonatkozásban tekintélyes képességekkel rendelkezik, amelyeket egyaránt kihasználnak az amerikai, orosz és kínai titkosszolgálatok, hogy digitális műveleti képességeiket hosszú távra kialakítsák. És ehhez még csak sok pénzre sincs szükség! A környezeti intelligencia elleni támadások ugyanis sokkal olcsóbbak egy katonai csapásnál. Egy olyan politika számára, amely politikai céljainak elérése érdekében az ilyen intézkedéseket a katonai erőszak klasszikus kellékei nélkül alkalmazza, a hibrid támadások a politika eszközeivé lesznek. Aki a háborút így értelmezi, újradefiniálja annak jelentését."

– *Választási titkok*: Ha már ármány és informatika, és még választás is, szinte az lenne a meglepő, ha nem a 2016-os USA-elnökválasztást hoznák fel, ahogy Hofstetter már előbb is tette. „A CIA felfigyelt az oroszok amerikaiak elleni cybertámadására, amely agresszivitás és intenzitás tekintetében mindent felülmúlt, amit eddig a régi ellenségtől a szovjet időkből szokványos politikai beavatkozásaként megszoktak. Az oroszok feltérképezték az amerikai választási infrastruktúrát, és megfigyelték az állami rendszereket. ... Az online behatolás arra enged következtetni, hogy Oroszország olyan támadásra készül, amely meglepi majd ez Egyesült Államokat. Elképzelhető volna, hogy az orosz kormány távirányítással úgy tudja befolyásolni az amerikai elnökválasztást, hogy az általuk óhajtott jelölt, Donald Trump kerekedjen felül? Mindenesetre abból kell kiindulni, hogy csak a gyengébb támadásokat fedezték fel. Kína mellett mégiscsak Oroszország rendelkezik a világ legprofesszionistább és leggyorsabb hekkereivel." – Felettébb érdekes! Az egész negyedik ipari forradalom minden alapvető informatikai innovációja Amerikában született, Amerika kétségkívül bővelkedik a legjobb informatikai szürkeállományban, övé a világ legerősebb hadserege, s a kiberhadviselés már nyilvánvalóan ott is elsőrangú fegyvernem, szoros szövetségese az informatikai innovációkban szintúgy élenjáró Izrael is, és mindemellett gyenge lenne profi hekkerekben?

Megjelenik ugyanakkor egy kívülállónak roppant meglepő szál is: „Bekapcsolódott a vizsgálatba a Jeh Johnson belbiztonsági miniszter vezetése alatt álló Department of Homeland Security is. Johnson sorra hívta a szövetségi államokat, hogy felajánlja segítségét a választási intézmények védelméhez, valamint a sebezhető pontok felderítéséhez. A szövetségi államok reakciója azonban mereven elutasító, sőt felháborodott. 'Gondoskodjon róla, hogy a washingtoni kormány távol tartsa magát az államunkban jelentkező választási problémáktól', hangzik az illetékes hivatalnokok ingerült válasza. Bizalmatlanok. Attól tartanak, Washington esetleg megpróbál beavatkozni a szövetségi ügyeikbe. A növekvő bizalmatlanság légkörében az amerikai szövetségi államok és hatóságaik körében ekkor az a gyanú kap lábra, hogy Washington maga avatkozik be az amerikai választási rendszerekbe és sérti meg integritásukat, hogy afféle partizánháború során fejtsen ki ellenállást a republikánus elnökjelölttel, Donald Trumppal szemben. Utóbbi pedig, ahelyett, hogy indítványozná egy külhatalom nyilvánvalóan ellenséges szándékú támadásának felderítését, a két elnökjelölt második televíziós vitája során e kijelentésre ragadtatja magát: 'Talán nem is volt hekkertámadás.' Ez belpolitikai megközelítésben: katasztrófa – s már csak ezért is jól érzékelteti a kívülről végrehajtott digitális támadás előnyeit. Az ilyet egész egyszerűen nem veszik komolyan – vagy gyorsan kétségbe vonják, hogy megtörtént. Bárki elindíthatta ugyanis az attakot, akár az ellenfél választási küzdelmét szervező team is – belföldről. Annak végül is minden oka megvan rá, hogy a személyt, aki egy rövid időre a másik politikai tábor exponense, minden

eszközzel hátráltassa, immár nemcsak politikai eszközökkel, hanem megkérdőjelezhető és illegális digitális befolyás érvényesítésével fizikailag és lélektanilag is."

S ez az a pont, ahol a látható háború a karakterszámlálóval térdre kényszerít. Jó olvasást a továbbiakhoz: roppant izgalmas, tanulságos, és nem kevéssé félelmetes!

Dr. Osman Péter